In the claims:

Following is a complete set of claims as amended with this Response.

1. (Original) A method comprising:

receiving a first request comprising a session identifier (I.D.);

assigning a unique I.D. to the first request;

selecting one of a plurality of servers to process the first request;

assigning the unique I.D. to the selected server; and

sending the first request to the server.

2. (Currently Amended) A method as in claim 1, additionally comprising:

subsequently receiving a second request comprising the session I.D.;

selecting the server that the unique ~~session~~ I.D. is assigned to; and

sending the second request to the selected server.

A3

3. (Currently Amended) A method as in claim 1, wherein said selecting one of a plurality of servers to process the first request comprises using a load balancing algorithm to determine a server to send the first request to.

4. (Original) A method comprising:

receiving a first request comprising a session identifier (I.D.);

selecting one of a plurality of servers to process the first request;

mapping the session I.D. to the selected server;

sending the first request to the selected server;

subsequently receiving a second request comprising the session I.D.;

determining that the second request comprises secure information;

selecting the server that the session I.D. is assigned to; and

sending the second request to the server.

5. (Original) A method as in claim 4, wherein the server is identified by an SSL (Secure Sockets Layer) context.

6. (Original) A method as in claim 4, wherein said selecting one of a plurality of servers to process the first request comprises using a load balancing algorithm to determine a server to route the first request to.

7. (Original) A method as in claim 4, additionally comprising:

determining that the second request comprises non-secure information; and

using a load balancing algorithm to determine a server to route the second request to.

#3

8. (Original) A method comprising:

receiving a first request comprising a session identifier (I.D.);

selecting one of a plurality of servers to process the first request, the server having a unique SSL (Secure Socket Layer) context, and the unique SSL context being associated with an SSL tunnel;

mapping the session I.D. to the selected SSL context;

sending the first request to the selected server;

subsequently receiving a second request comprising the session I.D.;

determining that the second request comprises secure information;

selecting the SSL context that the session I.D. is assigned to; and

sending the second request to the server via the SSL tunnel associated with the SSL context.

9. (Original) A method as in claim 8, wherein said selecting one of a

plurality of servers to process the first request comprises using a load balancing algorithm to determine a server to route the first request to.

10. (Original) A method as in claim 8, additionally comprising:

determining that the second request comprises non-secure information; and

using a load balancing algorithm to determine a server to route the second request to.

11. (Currently Amended) A method comprising:

receiving a request comprising a session identifier (I.D.);

#3 determining if the session I.D. is associated with an SSL (Secure Sockets Layer) context;

determining if the request is associated with a secure transaction;

if no session I.D. is associated with an SSL context, then selecting one of a plurality of servers to process the first request, the server having a unique SSL (Secure Socket Layer) context, and the unique SSL context being associated with an SSL tunnel; and

if the request is associated with a secure transaction, then:

mapping the session I.D. to the selected SSL context; and

sending the ~~second~~ request to the server via the SSL tunnel associated with the SSL context.

12. (Original) A method as in claim 11, wherein said selecting one of a plurality of servers to process the request comprises using a load balancing algorithm to determine a server to route the request to.

13. (Original) A method as in claim 11, wherein said determining if the

request is associated with a secure transaction comprises determining if an SSL packet is associated with the request.

14. (Original) A method as in claim 11, wherein said determining if the session I.D. is associated with an SSL (Secure Sockets Layer) context comprises looking up the session I.D. in a mapping table to determine if the mapping table comprises an entry for the session I.D. and a corresponding SSL context.

15. (Original) A system comprising a dispatching processor unit to:

receive a first request comprising a unique session identifier (I.D.);

select a server from a plurality of servers to process the request;

assign the unique session I.D. to the selected server, and store the unique session I.D. and corresponding identifier for the selected server in a mapping table comprising entries of session I.D.s each having a corresponding server identifier;

send the first request to the selected server;

receive a second request comprising the unique session I.D.;

find the unique session I.D. in the mapping table; and

send the second request to the server corresponding to the unique session I.D. in the mapping table.

16. (Original) A system as in claim 15, wherein a preexisting SSL (Secure Sockets Layer) tunnel exists between the dispatching processor unit and the selected server, the SSL tunnel being identified by an SSL context, and the mapping table comprising entries of session I.D.s each having a corresponding SSL context.

17. (Original) A system as in claim 15, wherein the dispatching processing unit selects one of a plurality of servers to process the request by using a load balancing

algorithm to determine a server to route the request to.

18. (Original) A system as in claim 17, wherein the dispatching processing unit uses a load balancing algorithm to determine a server to route the request to by employing a load balancer.

19. (Original) A system comprising:

a dispatching processor unit to:

send client requests to a plurality of servers in a server farm;

receive a client request comprising a session identifier (I.D.);

A3

determine if state information associated with the session I.D. already exists on one of a plurality of servers in the server farm;

send the client request to the server if the state information already exists on a server; and

employ a load balancer to determine one of the servers to send the client request to if the state information does not already exist on a server;

a load balancer in communication with the dispatching processor unit to determine one of a plurality of servers to send the client request to; and

a quality of service (QoS) manager in communication with the dispatching processor unit to decide which one of multiple client requests is processed if multiple client requests are sent to the same server.

20. (Original) A system as in claim 19, wherein the dispatching processor unit determines if state information associated with the session I.D. already exists on one of a plurality of servers in a server farm by searching a mapping table comprising a session I.D. mapped to a server.

21. (Original) A system as in claim 20, wherein the session I.D. is mapped to a server by the session I.D. being associated with an SSL (Secure Sockets Layer) context, and the SSL context is associated with the server.

22. (Original) A machine-readable medium having stored thereon data representing sequences of instructions, the sequences of instructions which, when executed by a processor, cause the processor to perform the following:

receive a first request comprising a session identifier (I.D.);

select one of a plurality of servers to process the first request;

map the session I.D. to the selected server;

A3

send the first request to the selected server;

subsequently receive a second request comprising the session I.D.;

determine that the second request comprises secure information;

select the server that the session I.D. is assigned to; and

send the second request to the server.

23. (Original) A medium as in claim 22, wherein the server is identified by an SSL (Secure Sockets Layer) context.

24. (Original) A medium as in claim 22, wherein the processor selects one of a plurality of servers to process the first request by using a load balancing algorithm to determine a server to route the first request to.

25. (Currently Amended) A medium as in claim 22, the processor to additionally:

determine that the second request comprises non-secure information; and

use a load balancing algorithm to determine a server to route the second request to.